Programa Integral de Seguridad y Gestión de Riesgos

“Innovación en la Gestión de Riesgos de Seguridad Física y Digital”

Autor: Mauricio Alan Illera Díaz

ORCID ID: 0009-0001-1505-4170

Researcher ID: OSI-4768-2025

Licencia: Creative Commons BY-NC-SA 4.0

Evolución y Principios de la Seguridad Física

Contexto Histórico

La seguridad física ha experimentado una transformación significativa a lo largo del tiempo. Originalmente, las medidas de seguridad se centraban en la custodia y vigilancia, recurriendo principalmente a guardias y candados como métodos de protección. Con el paso de los años, este enfoque evolucionó hacia sistemas integrados que combinan controles físicos, técnicos y administrativos, adoptando el concepto de "defensa en profundidad" o capas de seguridad. Esta visión avanzada reconoce que una protección efectiva requiere un equilibrio entre prevención, detección, retraso y respuesta.

En las últimas tres décadas, el sector ha sido testigo de la estandarización y profesionalización del oficio. Han surgido organismos profesionales como ASIS, así como normas específicas para la cadena de suministro, tales como BASC, OEA/AEO, ISO 28000 y C-TPAT. Además, se han publicado guías gubernamentales como las del DHS/CISA y NPSA/ProtectUK. Estos marcos normativos y profesionales exigen la presencia de gobernanza, auditoría y formación continua, además de la integración de tecnología en los procesos de seguridad.

Las certificaciones internacionales de comercio y seguridad, entre las que destacan BASC, OEA/AEO, C-TPAT e ISO 28000, han dejado de ser simples distintivos; ahora requieren la implementación de controles físicos demostrables, trazabilidad, gestión documental y capacitación constante del personal. El cumplimiento de estos estándares contribuye a reducir la fricción en las cadenas de suministro internacionales.

Principios Actuales de la Seguridad Física

Defensa en profundidad: La protección se estructura en múltiples capas, de modo que la falla de una sola no resulte en la pérdida total de seguridad.

Enfoque basado en el riesgo y proporcionalidad: Las inversiones en seguridad se determinan considerando el impacto y la probabilidad de incidentes, reconociendo que no todos los sitios requieren el mismo nivel de protección.

Integración físico-digital: Los controles físicos y los sistemas de tecnología de la información se combinan, permitiendo la conexión de sistemas de control de accesos, registros y la correlación entre CCTV y logs.

Cultura y responsabilidad compartida: La seguridad efectiva depende de roles claros, formación adecuada y la medición de indicadores clave (KPIs), evitando la total externalización a proveedores.

Mauricio Alan Illera Diaz

Auditoría continua y mejora constante: Se realizan controles, revisiones y pruebas periódicas, tales como pruebas de penetración físicas, simulacros y auditorías tanto internas como externas.

Clasificación práctica: Áreas / Capas que TODO lugar debe cubrir

A continuación, te presento la lista clasificada (general) —cada línea es un dominio que debes evaluar y documentar (política + controles + KPIs). Puedes usar esto como checklist maestro:

Seguridad Perimetral

Infraestructura física

Se garantiza la total integridad del perímetro, asegurando que no existan roturas, huecos, oxidación ni deformaciones. La altura mínima de las barreras perimetrales es definida en función del nivel de riesgo, utilizando cercas reforzadas antiescala y antiderribo. Las mallas se mantienen sin cortes ni manipulación y se verifica la ausencia de objetos, muebles o estructuras que puedan facilitar el escalamiento. La iluminación es continua, sin zonas oscuras, y la señalización de áreas restringidas es visible y está actualizada.

Sistemas electrónicos

Se cuenta con sensores perimetrales operativos (microfónicos, IR, fibra óptica), alarmas que se prueban semanalmente y cámaras con visión de 180° o 360°, eliminando puntos ciegos. Los domos y housings son antivandálicos, y los sistemas de grabación (DVR/NVR) disponen de respaldo energético y redundancia para garantizar su funcionamiento.

Procedimientos

Las bitácoras de rondines se mantienen actualizadas, existen protocolos formales ante cualquier detección o violación del perímetro, y los mantenimientos trimestrales quedan debidamente documentados.

Controles de Acceso (Personal, Visitantes, Proveedores)

Tecnología y autenticación

El acceso se controla mediante torniquetes o puertas con biometría o RFID. Se lleva un registro digital de entradas y salidas, con verificación obligatoria de identidad y credenciales visibles, asignando permisos diferenciados según el perfil.

Gestión de visitantes y proveedores

Se exige pre-registro, validación de identificación oficial y acompañamiento durante la permanencia. Todas las herramientas y equipos son revisados tanto al ingreso como a la salida.

Acceso vehicular

Se utilizan barreras anti-ariete funcionales y lectores automáticos de placas, además de realizar una inspección vehicular completa con checklist.

Seguridad en CCTV

Diseño

El sistema cubre la totalidad de los puntos críticos, con una matriz de cámaras por área que elimina puntos ciegos y garantiza visión nocturna mediante IR o cámaras térmicas.

Calidad y almacenamiento

Las grabaciones tienen una resolución mínima de 1080p, con un almacenamiento garantizado de 30 días, respaldadas en nube o en servidores redundantes.

Operación

El monitoreo es 24/7, se mantiene una lista de eventos críticos de vigilancia y se realizan auditorías mensuales de funcionamiento y limpieza.

Seguridad en Oficinas Administrativas

Controles internos

Las oficinas permanecen aseguradas fuera de horario, con archiveros y cajones bajo llave, y la aplicación estricta de la política de escritorios limpios ("Clean Desk Policy").

Activos

Todos los dispositivos (laptops, etc.) están etiquetados y controlados. Los documentos sensibles se resguardan de manera segura y está prohibido el uso de USB no autorizados. Cada uno de los colaboradores firman una hoja de entrega de herramientas o equipo, donde hay que mencionar que ellos son los responsables del activo que la empresa le confía.

Seguridad de la Información (Física y Digital)

Accesos

Las sesiones se bloquean automáticamente, se exigen contraseñas robustas y autenticación multifactor (MFA), y los roles de acceso se asignan por jerarquía y necesidad.

Protección de datos

Los respaldos están protegidos y cifrados, los servidores ubicados en cuartos restringidos, y existen controles anti-malware y anti-filtración.

Infraestructura

Se dispone de UPS operativos, centros de datos con acceso biométrico y CCTV interno en los cuartos de servidores.

Seguridad en Bodegas y Centros de Distribución

Procesos operativos

Se controla la entrada y salida de mercancía mediante sellos numerados y auditados, y se realiza verificación cruzada entre pedido, carga y transportista.

Infraestructura

En las áreas de alta rotación hay vigilancia permanente, las puertas de emergencia son auditadas y los racks se mantienen sin obstrucción y respetando límites de peso.

Personal

Se aplica una separación de funciones clave, un estricto control de visitantes y supervisión directa en carga y descarga.

Seguridad en Patio de Maniobras

Vehículos

Todos los vehículos son inspeccionados con checklist, los sellos se verifican al ingreso y egreso, y el registro GPS permanece activo.

Operación

El perímetro se mantiene sin puntos de fuga, con iluminación extendida para maniobras nocturnas y supervisión CCTV en tiempo real.

Choferes

Existe un área de espera controlada y los choferes no tienen libre acceso a áreas internas.

Seguridad en Manufactura, Plantas y Fábricas

Personas

En las instalaciones de manufactura, plantas y fábricas, es obligatorio que todo el personal utilice el equipo de protección personal (EPP) adecuado para sus funciones. Además, la señalización de riesgos es clara y visible en todas las áreas de trabajo, lo que contribuye a la prevención de accidentes. El acceso a la maquinaria o a zonas peligrosas está restringido únicamente a personal autorizado, disminuyendo así el riesgo de incidentes laborales.

Procesos

Las máquinas operan con protecciones físicas instaladas para evitar el contacto accidental con partes móviles o peligrosas. Los paros de emergencia son sometidos a pruebas periódicas para asegurar su funcionamiento óptimo en caso de una contingencia. Asimismo, existe un control estricto sobre el uso y almacenamiento de herramientas, evitando pérdidas o usos indebidos.

Materiales

Las sustancias químicas son almacenadas de manera segura y conforme a la normativa, minimizando riesgos para el personal y el entorno. La materia prima de alto valor, por su importancia estratégica y riesgo de sustracción, cuenta con acceso restringido únicamente al personal autorizado.

Seguridad Interna / Intramuros

Cultura organizacional

La seguridad interna se fundamenta en una cultura organizacional donde los custodios asumen la responsabilidad por zonas asignadas. Es obligatorio reportar cualquier anomalía detectada en las áreas, y se llevan a cabo auditorías internas de manera semanal para asegurar el cumplimiento de los protocolos establecidos.

Prevención de pérdidas

Para reducir riesgos, se elaboran mapas de vulnerabilidad por zonas que permiten focalizar estrategias de control. Se implementan protocolos anti-hurto y se lleva un control documentado y sistemático tanto de merma como de scrap, lo que facilita la detección de desviaciones y la oportuna toma de decisiones correctivas.

Seguridad de Personal y Recursos Humanos

Procesos

La seguridad del personal inicia con la verificación de antecedentes antes de su contratación. En caso de bajas, se realiza una desvinculación segura retirando de inmediato todos los accesos físicos y digitales. Existen protocolos específicos para la gestión de comportamientos inadecuados, situaciones de acoso o violencia laboral.

Bienestar

Se promueven programas de salud emocional dirigidos al personal, así como canales confidenciales de denuncia, brindando atención oportuna y un entorno seguro para todos los colaboradores.

Seguridad de Documentación y Activos Críticos

Documentos

Los documentos estratégicos son resguardados en cajas fuertes y se restringe estrictamente su copia o escaneo, garantizando la protección de información sensible para la organización.

Activos

Se realizan inventarios mensuales de los activos críticos. Los contenedores utilizados cuentan con sellos inviolables, lo que asegura la integridad y control de los bienes almacenados.

Seguridad Contra Incendios

Infraestructura

La infraestructura de seguridad contra incendios incluye la instalación de detectores y alarmas funcionales en puntos estratégicos. Los extintores se encuentran vigentes, señalizados y distribuidos de manera accesible, y las rutas de evacuación permanecen siempre libres de obstáculos.

Operación

Se realizan simulacros de incendio cada seis meses, en los cuales el personal participa activamente y está capacitado en el uso de extintores y en el manejo de emergencias relacionadas con el fuego.

Seguridad en Proveedores y Contratistas

Cumplimiento

La gestión de proveedores críticos incluye la evaluación y validación de certificaciones tales como BASC, OEA o ISO, y la exigencia de escolta interna obligatoria para determinadas operaciones.

Operación

Como parte de los controles operativos se revisan mochilas, cajas y herramientas de proveedores y contratistas, además de prohibirse el acceso a zonas no autorizadas dentro de las instalaciones.

Seguridad en Transporte y Logística

Unidades

Las unidades de transporte están equipadas con GPS activo y botón de pánico funcional, y las rutas operativas se clasifican según el nivel de riesgo asociado.

Procesos

Se realiza monitoreo permanente de las rutas, existen protocolos específicos ante desvíos o emergencias, y el checklist de entrega y recepción debe ser firmado para asegurar la trazabilidad de la mercancía.

Gestión de Riesgos y Continuidad Operativa

Análisis

La gestión de riesgos inicia con la identificación de amenazas tanto internas como externas, y la posterior evaluación de vulnerabilidades físicas y humanas. Se elabora una matriz de criticidad de riesgos por cada instalación, lo que permite priorizar acciones preventivas.

Continuidad

El plan de continuidad de negocio y recuperación ante desastres (BCP/DRP) se mantiene actualizado. Además, se dispone de respaldo energético y sistemas redundantes, así como protocolos de contingencia específicos para cada tipo de evento.

Simulacros por tipo de riesgo

Se programan simulacros anuales para riesgos críticos como robo, incendio, intrusión o accidente, además de simulacros particulares por área (bodega, patio, oficinas), de evacuación y de emergencia médica. Todos los ejercicios consideran el registro puntual de tiempos, fallas y acciones de mejora implementadas.

Evidencia de riesgos

Se mantienen actualizados los mapas de riesgos, evidencias fotográficas de vulnerabilidades detectadas, reportes de incidencias clasificadas, registro de acciones de mitigación implementadas y auditorías internas y externas documentadas como parte de la gestión integral.

Seguridad en Áreas de Alto Valor

Infraestructura

En áreas de alto valor, los accesos son reforzados y se instala un sistema de videovigilancia dedicado que opera las 24 horas, los 7 días de la semana. El acceso se controla mediante sistemas biométricos, asegurando que sólo personal autorizado pueda ingresar.

Procesos

Para la apertura de estos espacios se requiere una doble verificación. Se realizan inventarios diarios y los sellos utilizados son numerados y auditados, garantizando un control riguroso de los activos.

Gestión Documental y Evidencias

Evidencia operativa

Las bitácoras operativas son digitales y centralizadas, los checklists son firmados y auditables, y todos los incidentes se reportan asegurando trazabilidad completa, lo que facilita el análisis y la toma de decisiones.

Cumplimiento normativo

Se revisan periódicamente los requisitos de cumplimiento, se realizan auditorías semestrales y la documentación se mantiene siempre actualizada y bajo estricto control, atendiendo los lineamientos de estándares internacionales como ASIS, BASC y OEA.

Proveedores, Contratistas (Regulatorio y Operativo)

Cumplimiento regulatorio y documental

Se cuenta con contratos vigentes con proveedores de seguridad, registro nacional de empresas de seguridad privada (cuando aplique), pólizas de responsabilidad civil y riesgos de trabajo, altas de IMSS del personal asignado, y se verifica la validez de permisos estatales y federales. El curriculum operativo de jefe de turno y supervisor es revisado, junto con la capacitación obligatoria y exámenes médicos, toxicológicos y psicométricos.

Control operativo

Se utilizan checklists de inicio y fin de turno, las rondas se validan digitalmente y el equipamiento es completo (radios, lámparas, uniforme, bitácoras). El proveedor es supervisado aleatoriamente, se revisan los tiempos de respuesta y se evalúan los KPIs.

KPI de proveedores de seguridad

Se mide la productividad y desempeño (% de rondines completados, incidencias detectadas, tiempo de respuesta, exactitud en reportes, ausentismo y rotación de personal, cumplimiento en capacitación). En cumplimiento legal se verifica la

documentación vigente y los permisos, así como la eficacia operativa y la satisfacción del servicio mediante evaluaciones mensuales internas y del cliente.

Gestión de Riesgos y Continuidad Operativa (Simulacros y Evidencias)

Simulacros por tipo de riesgo

Se realiza al menos un simulacro anual por cada riesgo crítico identificado (robo, incendio, intrusión, accidente), y simulacros específicos por área. Se incluyen simulacros de evacuación y de emergencia médica, y en empresas logísticas, simulacros de robo con violencia. Se documentan tiempos, fallas y acciones de mejora.

Evidencia de riesgos

Se mantienen mapas de riesgos actualizados, evidencias fotográficas, reportes de incidencias clasificadas, evidencias de mitigación y auditorías internas y externas.

Análisis del Entorno, Riesgo Social y Crimen Cercano

Evaluación del contexto externo

Se analiza la incidencia de delitos en un radio de 1 a 5 km, registrando eventos como asaltos, robos a transporte, comercio, vehículos, instalaciones vecinas, intentos de intrusión, riñas, presencia de grupos delictivos y vandalismo.

Fuentes de información

Se utilizan reportes policiales, mapas delictivos, alertas vecinales, chats empresariales de seguridad, reportes ciudadanos, cámaras C5 cuando existan y coordinación con Seguridad Pública local.

Indicadores sociales

Se mide la frecuencia de delitos por semana o mes, clasificación por tipo, horarios de mayor riesgo, zonas externas más vulnerables, riesgos por perfil social y proyección de riesgo a corto plazo.

Controles derivados

Estos incluyen refuerzo de accesos en horarios críticos, supervisión externa con CCTV perimetral, comunicación con vecinos y parques industriales, rutas alternativas y protocolos de cierre por riesgo extremo.

Identificación y Clasificación de Riesgos Naturales

Tipología de riesgos

Se consideran sismos, inundaciones, lluvias intensas, huracanes, derrumbes, granizadas, ondas de calor y bajas temperaturas extremas, incendios forestales cercanos, fallas eléctricas masivas, sequías y riesgo volcánico según la región.

Variables de evaluación para matriz

Cada riesgo es evaluado en función de su probabilidad histórica, severidad del impacto, zonas vulnerables, servicios críticos afectados, tiempo estimado de interrupción, capacidad de respuesta, controles existentes y faltantes.

Evidencias requeridas por estándares (BASC / OEA / ISO / ASIS)

BASC

Se mantiene un mapa de riesgos ambientales actualizado, registro de afectaciones históricas, controles preventivos, simulacros y comprobación de alarmas y rutas.

OEA

Se cuenta con matriz de riesgo ambiental, procedimientos de continuidad operativa, bitácoras de fallas por clima, protocolos de recuperación y pruebas de resiliencia de la cadena de suministro.

ISO 28000

Se realiza un análisis integral de amenazas externas, evaluación de vulnerabilidades, reportes de mantenimientos, indicadores de impacto y procedimientos para clima extremo.

ASIS (PSP / APP / CPP)

Incluye análisis de amenazas naturales, evaluación por capas, programas de prevención, ejercicios de resiliencia y pruebas de capacidad ante cortes eléctricos o de red.

Simulacros y ejercicios obligatorios

Tipos de simulacros

Se programan simulacros de sismo, evacuación por inundación o incendio, respuesta ante corte eléctrico, evacuación por derrumbe, punto de reunión seguro y continuidad operativa sin comunicaciones.

Evidencias

Se documentan actas firmadas, fotos, listas de participación, tiempos de evacuación, áreas con fallas detectadas y acciones de mejora.

Controles y Mitigaciones

Infraestructura

Se asegura el desazolve mensual de desagües, la prueba semanal de plantas de emergencia, UPS en nodos críticos, sellado de áreas, señalización climática y revisión de estructura.

Documentos requeridos

Incluyen Plan de Continuidad y Contingencia (PCC/PTRA), manual de respuesta a emergencias, mapas de evacuación, plan de resiliencia de la cadena de suministro, bitácora de clima severo, mantenimiento preventivo documentado y contratos con proveedores de emergencia.

Integración con Proveedores

Guardias, custodios y tecnología

Los proveedores cuentan con procedimientos de evacuación y capacitación en emergencias naturales, evidencias de asistencia, mano de obra suficiente para contingencias y cumplimiento legal en materia de Protección Civil. Para los proveedores de transporte y custodia, se evalúan rutas con riesgo climático, protocolos para detener operaciones, bitácoras de afectaciones y comunicación continua con C4/C5. Los proveedores de CCTV y tecnología disponen de planes de respaldo eléctrico, evidencias de pruebas y control de fallas por tormenta.

Análisis del entorno social relacionado

Como parte del riesgo, se consideran robos a transeúntes durante evacuaciones, intrusiones aprovechando apagones, asaltos durante tormentas, delincuencia oportunista tras sismos o desastres, zonas “rojas” al evacuar y los incidentes del barrio de los últimos seis meses.

Lista de Verificación de Seguridad Multinivel

Perímetro y entorno exterior

(Objetivo: dificultar el acceso no autorizado, detectar intrusos y mantener visibilidad)

Lista de verificación

- ✓ ¿Existe un plano perimetral actualizado con zonas y puntos críticos?
- ✓ Barreras físicas: vallas/muros en buen estado, altura mínima definida, sin apuntalamientos ni escalones.
- ✓ Bollards y protección vehicular en accesos principales y zonas sensibles.
- ✓ Control y poda de vegetación: línea de visión libre de 3–5 m según riesgo.
- ✓ Iluminación perimetral: lux medido, cobertura sin sombras en accesos y rutas peatonales.
- ✓ Señalización visible: propiedad privada, CCTV en operación, zonas restringidas.
- ✓ Detección perimetral: sensores PIDS, cercas eléctricas o sensores de vibración instalados y testeados.
- ✓ Rutas de patrulla definidas y bitácora de rondines (horario, operador, hallazgos).
- ✓ Entradas secundarias/servicios: identificadas, cerradas y con control igual que entrada principal.
- ✓ Documentación de obras o proveedores que afectan el perímetro (planos, permisos).
- ✓ Evidencia mínima
- ✓ Plano perimetral firmado; registros de mantenimientos; pruebas de sensor (logs).
- ✓ Informe de medición de iluminación (lux).
- ✓ Rondas firmadas y registro de hallazgos.
- ✓ KPIs sugeridos
- ✓ % de rondas realizadas vs planificadas; tiempo medio de resolución de hallazgos perimetrales.

B — Controles de acceso (personas y vehículos)

(Objetivo: autorizar, auditar y controlar entradas/salidas con trazabilidad)

Lista de verificación

- ✓ Políticas de acceso documentadas (tipos de credenciales, vigencia, proceso de revocación).
- ✓ Sistema de control de acceso (ACM): integración con HR, logs centralizados, backup.
- ✓ Credenciales: emisión con foto, codificación (badges), proceso de recuperación/evitación de suplantación.
- ✓ Torniquetes/torres de control para accesos principales; control vehicular con barrera y registro de placas.
- ✓ Proceso de visitantes: preregistro electrónico, identificación, escort obligatorio en zonas restringidas.
- ✓ Gestión de contratistas: permisos temporales, verificación de antecedentes y seguro vigente.
- ✓ Doble control en zonas críticas (two-person rule, escort, o biometría + badge).
- ✓ Procedimientos de salida de materiales/personas (sign-out, autorización, revisión física aleatoria).
- ✓ Interlocks y failsafes para puertas críticas (no dejar puertas abiertas por tiempos > X segundos).
- ✓ Integración con CCTV y con sistema de alarmas (eventos de acceso generan tags en video).
- ✓ Evidencia mínima
- ✓ Logs de acceso exportables (fecha, hora, usuario, tarjeta), políticas HR vinculadas y registros de revocación.
- ✓ Registros de visitantes y contratistas con documentación adjunta.
- ✓ KPIs sugeridos
- ✓ % de accesos no autorizados detectados; tiempo medio de revocación de credenciales tras salida.
- ✓ (Soporte conceptual y guías de implementación: prácticas de control de accesos y defensa en profundidad).

C — Seguridad en muelles y patio de maniobra (recepción y despacho)

(Objetivo: prevenir pérdida durante manipulación, carga/descarga y transporte)

Lista de verificación

- ✓ Zonas definidas: zona limpia de recepción, zona de inspección, muelle cerrado para carga crítica.
- ✓ Control vehicular: identificación del vehículo, verificación de chofer (ID), pre-check de contenedores/sellos.
- ✓ Sellos contables: utilización de sellos numerados, registro de número de sello y verificación en entrega.
- ✓ Procedimiento de inspección de carga: checklist de embalaje, reconciliación con documentos.
- ✓ Cámara dedicada en cada muelle/andén con cobertura del interior del camión/contendedor (ángulo + NVR).
- ✓ Horarios de operación y control de acceso para proveedores (ventanillas horarias).
- ✓ Precintos y cadena de custodia: registro de quién recibió, quién entregó, hora y firma.
- ✓ Área de espera para conductores fuera de zona restringida; acompañamiento por personal autorizado.
- ✓ Control de cargas salientes: autorización por jefe de almacén + verificación física.
- ✓ Procedimiento ante anomalías: retención, bloqueo, investigación y notificación a seguridad corporativa.
- ✓ Evidencia mínima
- ✓ Registros de entrada/salida (manifiestos) escaneados y firmados; fotos de precintos/sellos en el log del muelle.
- ✓ Video de muelle retenido por período definido.
- ✓ KPIs sugeridos
- ✓ % de discrepancias detectadas vs volumen; tiempo medio para aceptar/rechazar una recepción.
- ✓ (Esto es crítico para programas BASC/OEA y controles de cadena de suministro).

D — Almacén / nave (intramuros, picking, inventario)

(Objetivo: proteger stock, limitar oportunidades de hurto interno y mejorar trazabilidad)

Lista de verificación

- ✓ Zonificación por niveles: pública → semirrestringida → restringida → crítica.
- ✓ Accesos a pasillos y estanterías controlados (tarjeta/biometría en áreas críticas).

- ✓ Políticas de picking: pick-to-verify (firma o scan por operador + supervisor), doble verificación en cargas críticas.
- ✓ Inventarios cíclicos programados y registros de conciliación (frecuencia basada en rotación e impacto).
- ✓ Controles en picking de alto valor: cámaras dedicadas, registro de operario, cierre de puertas temporales.
- ✓ Control de devoluciones y ajustes: proceso documentado, autorización y investigación de excepciones.
- ✓ Gestión de residuos y empaques: control de cajas vacías que puedan contener bienes.
- ✓ Etiquetado y trazabilidad (RFID/Barcode) con verificación en cada transferencia interna.
- ✓ Procedimientos de seguridad para entradas nocturnas/turnos rotativos (especial atención a personal solitario).
- ✓ Mantenimiento de estanterías y comprobación de accesos de emergencia y rutas de evacuación.
- ✓ Evidencia mínima
- ✓ Logs de picking y conciliaciones; registros de inventario con firmas; tickets de ajuste por investigación.
- ✓ KPIs sugeridos
- ✓ Shrinkage mensual; % cumplimiento inventarios; tasa de ajustes por operador.

E — CCTV, sala de control y gestión de imágenes

(Objetivo: disuadir, detectar y proporcionar evidencia usable)

Lista de verificación

- ✓ Diseño por objetivo: identificación de objetivos (deterrence/detection/forensic) y mapa de cámaras por objetivo.
- ✓ Cobertura: sin puntos ciegos en accesos, muelles, zonas de alto valor; se utiliza regla de framing (target ≈ 10% del alto de la pantalla para detección).
- ✓ Resolución mínima por propósito (p.ej. 1080p para reconocimiento, 4K para forense en zonas críticas) y lentes adecuados.
- ✓ Iluminación IR y WDR donde aplica; pruebas nocturnas y condiciones mixtas.
- ✓ Retención: política documentada (ej.: 30 días por defecto salvo requisitos legales), capacidad NVR/archivado y cifrado de archivos.
- ✓ Control room: acceso restringido, personal entrenado, SOPs de monitoreo, bitácora de operadores y auditorías de operadores.

- ✓ Integración: eventos de acceso/alarma ligados a marcadores en video (tagging automático).
- ✓ Mantenimiento: plan de revisiones (lentes limpias, firmware, sincronización de hora, health checks).
- ✓ Privacidad y señalética: evaluación de impacto en protección de datos, avisos visibles y reducción de retención cuando no es necesario.
- ✓ Procedimiento de extracción de evidencia: chain-of-custody documentado, hashes, copias autorizadas.
- ✓ Evidencia mínima
- ✓ Plano de cámaras con finalidad; logs de mantenimiento; política de retención; registros de acceso a video.
- ✓ KPIs sugeridos
- ✓ % de cámaras con estado OK; tiempo de recuperación de video requerido por investigación.
- ✓ (Guías técnica y buenas prácticas: ProtectUK / DHS CCTV Tech Handbook).

F — Sistemas de alarma, detección temprana y respuesta

(Objetivo: alertar y activar la respuesta correcta con playbooks definidos)

Lista de verificación

- ✓ Integración de sensores (intrusión, humo, agua, temperatura) a una plataforma única (preferible).
- ✓ Zonas de alarma mapeadas y clasificacion por prioridad.
- ✓ Procedimientos de verificación de alarmas (2º verificación, video-check antes de despachar).
- ✓ Contactos de respuesta internos y externos (policía privada, policía municipal, bomberos) con SLA definidos.
- ✓ Playbooks por incidente (hurto, intrusión nocturna, incendio, toma de rehenes, falla crítica).
- ✓ Registros y after-action report para cada incidente; lecciones aprendidas integradas.
- ✓ Pruebas periódicas (sistemas y ejercicios full-scale) documentadas.
- ✓ Evidencia mínima
- ✓ Playbooks firmados; registros de incidentes y reporte de pruebas.
- ✓ KPIs sugeridos
- ✓ Tiempo medio de verificación; tiempo medio de respuesta; % de alarmas falsas.

G — Seguridad en oficinas y administración

(Objetivo: proteger información física y personal administrativo)

Lista de verificación

- ✓ Control de accesos interior (zonas administrativas con credenciales independientes).
- ✓ Clean-desk policy y políticas de almacenamiento de información sensible (cajas fuertes, archivo bajo llave).
- ✓ Gestión de visitantes (áreas de espera definidas y escort).
- ✓ Procedimiento de destrucción segura (shredding certificado) para documentos.
- ✓ Protección de salas de reuniones y salas de server (tarjeta + registro).
- ✓ Señalética y políticas visibles sobre uso de dispositivos personales en áreas sensibles.
- ✓ Evidencia mínima
- ✓ Política clean-desk; registros de destrucción; listas de acceso a salas críticas.
- ✓ KPIs sugeridos
- ✓ Incidentes de exposición de información física; % cumplimiento clean-desk.

H — Seguridad de la información (intersección it / ot)

(Objetivo: evitar que un acceso físico cause un impacto digital y viceversa)

Lista de verificación

- ✓ Controles físicos en salas IT/OT: puertas con control, registro de acceso, CCTV redundante.
- ✓ Segregación de redes OT/IT y control de endpoints en zonas industriales.
- ✓ Integración de logs: accesos físicos, eventos CCTV y logs de red en un SIEM o plataforma de correlación.
- ✓ Gestión de credenciales y privilegios para acceso a sistemas críticos (principio de menor privilegio).
- ✓ Backups offline de sistemas críticos y pruebas periódicas de restauración.
- ✓ Procedimientos de cambio (change management) con revisión de seguridad.
- ✓ Evidencia mínima
- ✓ Registros de acceso a sala de servidores; política de segregación; logs integrados.
- ✓ KPIs sugeridos

- ✓ Número de correlaciones físico→digital detectadas; % de parches aplicados en ventana.

I — Personal, selección, formación y cultura

(Objetivo: reducir riesgo humano mediante selección, formación y responsabilidad compartida)

Lista de verificación

- ✓ Proceso formal de contratación: verificación de antecedentes, referencias y evaluaciones previas.
- ✓ Programas de inducción y formación periódica (robos internos, fraude, uso de credenciales, conducta).
- ✓ Evaluaciones periódicas y monitoreo de desempeño; control de rotación y periodos de prueba.
- ✓ Protocolos de control para roles sensibles (doble verificación, separación de funciones).
- ✓ Programas de incentivos y reconocimientos por cumplimiento (KPIs de disciplina).
- ✓ Procedimiento y política ante denuncias internas (canal confidencial).
- ✓ Contratos con cláusulas de seguridad para contratistas.
- ✓ Evidencia mínima
- ✓ Registros de formación por persona; resultados de verificaciones; contratos con cláusulas.
- ✓ KPIs sugeridos
- ✓ % personal verificado; % personal formado; incidentes atribuidos a fallo humano.
- ✓ (Importante para BASC/OEA: evidencia de formación y selección).

J — Llaves, candados y gestión de custodia

(Objetivo: controlar la posesión física de medios de acceso y llaves)

Lista de verificación

- ✓ Inventario de llaves y credenciales (registro maestro con responsable y ciclo de vida).
- ✓ Política de duplicados: prohibido duplicar sin autorización, registro de petición y devolución.
- ✓ Armarios de llaves con control (caja fuerte o key cabinet con logs).

- ✓ Procedimiento para pérdida/robo de llaves: revocación inmediata y cambio de cerraduras si aplica.
- ✓ Control de llaves maestras (custodia dual y registro de uso).
- ✓ Evidencia mínima
- ✓ Registro maestro y bitácora de emisión/devolución; evidencias de incidentes por llave.
- ✓ KPIs sugeridos
- ✓ Número de eventos por llave perdida; tiempo de revocación.

K — Gestión documental, auditoría y kpis

(Objetivo: gobernanza, trazabilidad y mejora continua)

Lista de verificación

- ✓ Manual de seguridad y políticas actualizadas y firmadas por dirección.
- ✓ Matriz de responsabilidades (RACI) por área/activo.
- ✓ Auditorías internas periódicas con plan de corrección y evidencia de cierre.
- ✓ Registros electrónicos (logs centralizados) con backup y retención.
- ✓ Dashboard de KPIs: incidentes, shrinkage, cumplimiento, tiempo respuesta.
- ✓ Plan documentado de mejora continua y lista de proyectos priorizados por riesgo/ROI.
- ✓ Evidencia mínima
- ✓ Informes de auditoría; dashboards exportables; registros de cierre de hallazgos.
- ✓ KPIs sugeridos
- ✓ % controles conformes; tiempo medio cierre hallazgo; shrinkage.

L — Continuidad, resiliencia y emergencias

(Objetivo: asegurar operación mínima y recuperación rápida)

Lista de verificación

- ✓ Plan de continuidad (BCP) y recuperación ante desastres (DRP) documentados.
- ✓ Redundancia de energía para áreas críticas (UPS, generador) y pruebas de corte programadas.
- ✓ Rutas alternativas para cadena de suministro y lista de proveedores críticos.
- ✓ Contactos de emergencia actualizados (autoridades, proveedores, respuesta médica).
- ✓ Ejercicios de mesa y simulacros con evaluación posterior (after-action).

- ✓ Evidencia mínima
- ✓ BCP/DRP firmados; registros de pruebas de conmutación; after action reports.
- ✓ KPIs sugeridos
- ✓ Tiempo objetivo de recuperación (RTO) vs real; % ejercicios completados.

M — Cumplimiento, privacidad y asuntos legales

(Objetivo: operar dentro del marco legal y proteger datos personales)

Lista de verificación

- ✓ Evaluación de impacto privacidad para CCTV y tratamiento de datos.
- ✓ Señalética y consentimiento cuando aplique; políticas de acceso a grabaciones.
- ✓ Cumplimiento local en materia laboral sobre vigilancia y horarios de trabajo.
- ✓ Revisión contractual y seguros (coberturas por pérdida, responsabilidad).
- ✓ Archivo y conservación documental conforme a normativas fiscal/aduaneras si aplica.
- ✓ Evidencia mínima
- ✓ DPIA o evaluación de impacto; cláusulas contractuales; pólizas vigentes.
- ✓ KPIs sugeridos
- ✓ Número de no conformidades legales; tiempo de respuesta a solicitudes de acceso a datos.
- ✓ ---
- ✓ Cómo usar este checklist en auditorías (sugerencia operativa)
- ✓ Traduce cada ítem en una pregunta de auditoría (Sí/No/NA) con evidencia requerida (foto, log, documento).
- ✓ Asigna riesgo a cada hallazgo (Bajo/Medio/Alto) y propietario para remediación.
- ✓ Prioriza correcciones por impacto y facilidad de implementación (quick wins: control de muelles, llaves, visitors).
- ✓ Registra todo en un sistema de gestión y haz un seguimiento semanal hasta cierre.

Innovación en la Gestión de Riesgos de Seguridad Física y Digital

Introducción

En el contexto actual, caracterizado por la transformación acelerada de los entornos operativos y la transición hacia infraestructuras híbridas que combinan componentes físicos, humanos y digitales, la gestión de riesgos ha evolucionado para requerir precisión, velocidad y adaptación continua. Los modelos tradicionales de manejo de riesgos, fundamentados en evaluaciones periódicas, resultan insuficientes frente a amenazas que cambian de forma significativa en cuestión de minutos. Este capítulo introduce un modelo de inteligencia de riesgo continua, apoyado en fuentes OSINT, inteligencia artificial y analítica avanzada, con el propósito de generar una visión de riesgo en tiempo real.

Objetivo

El objetivo es establecer un modelo integral de gestión del riesgo capaz de anticipar, detectar y mitigar amenazas en tiempo real. Esto permite reducir pérdidas, mejorar la capacidad de respuesta y adaptarse dinámicamente a entornos altamente volátiles.

Desarrollo

Limitaciones del modelo tradicional

Los diagnósticos de seguridad física y digital basados en inspecciones trimestrales o anuales generan ventanas de vulnerabilidad, pues entre cada evaluación se presentan cambios significativos en el entorno. Estos incluyen modificaciones urbanas, desplazamientos o incrementos en actividades delictivas, ajustes operativos, alteraciones en horarios y la incorporación de nuevos proveedores, así como el surgimiento de nuevas modalidades de ataque físico y digital. El desfase temporal entre evaluaciones propicia la toma de decisiones críticas con información obsoleta.

Transición hacia un modelo dinámico

El nuevo paradigma de gestión de riesgos se fundamenta en la monitorización permanente, donde la información fluye y se procesa de manera continua. Esto se logra mediante:

Fuentes OSINT: Se monitorean redes sociales con enfoque contextual, se consultan noticias locales y nacionales en tiempo real, se emplean aplicaciones ciudadanas para el reporte de delitos y se utilizan mapas policiales y tendencias geoespaciales, además de plataformas de tráfico, movilidad y emergencias.

Inteligencia Artificial: Herramientas de IA generativa y modelos de machine learning permiten identificar patrones emergentes, detectar anomalías en el comportamiento ambiental, predecir amenazas con base en correlaciones históricas y reclasificar riesgos automáticamente.

Dashboards en tiempo real: Los sistemas presentan alertas priorizadas según el nivel de criticidad, mapas de calor actualizados segundo a segundo, información sobre riesgo dinámico por activo, ruta o persona, e indicadores predictivos del entorno.

Caso de estudio: logística en Michoacán

Una empresa con rutas en zonas de conflicto implementó este modelo dinámico. La inteligencia artificial detectó un aumento anormal en publicaciones ciudadanas sobre bloqueos. Paralelamente, el análisis histórico evidenció que los picos de tensión social antecedían cierres carreteros. Como resultado, se generó una alerta seis horas antes del evento, lo que permitió desviar unidades, reprogramar entregas y evitar pérdidas valoradas en 2.3 millones de dólares.

Integración con la toma de decisiones

El sistema propuesto sugiere respuestas automatizadas y adaptables, tales como recalcular rutas seguras, activar protocolos de protección de personal, notificar a clientes de manera transparente y escalar incidentes automáticamente.

Alcance

Este modelo es aplicable a sectores como logística y transporte, retail y distribución, energía y minería, infraestructura crítica, así como operaciones urbanas o rurales de alto riesgo.

Conclusión

El riesgo en la actualidad es dinámico y la capacidad de una organización para anticipar amenazas en tiempo real determina su resiliencia. Adoptar este modelo no solo contribuye a la reducción de incidentes, sino que transforma la seguridad en una ventaja competitiva fundamentada en agilidad, precisión y anticipación.

Amenazas Híbridas: Cuando lo Físico y lo Digital se Atacan Juntos

Introducción

En los entornos industriales, logísticos y corporativos, la interconexión es cada vez mayor y las fronteras entre la ciberseguridad y la seguridad física se desdibujan. Esto da lugar a amenazas más complejas, conocidas como ataques híbridos, en los cuales lo físico y lo digital se combinan y operan simultáneamente. Este capítulo aborda la identificación, modelado y mitigación de estas amenazas de nueva generación.

Objetivo

El objetivo es desarrollar un modelo que permita comprender, anticipar y neutralizar amenazas que combinan intrusión física, sabotaje, ingeniería social, manipulación de sistemas OT/IT y ataques digitales coordinados.

Desarrollo

Naturaleza de las amenazas híbridas

Un ataque híbrido actúa en varias capas:

Física: incluye intrusión, robo, sabotaje y plantación de dispositivos.

Digital: involucra malware, manipulación de logs y desactivación de sensores.

Humana: se vale de ingeniería social avanzada, uso de deepfakes y coerción.

La peligrosidad de estos ataques reside en que cada vector de ataque refuerza los demás.

Modos de operación más frecuentes

Robo con deepfake: Ejemplo de incidentes en los que un atacante utiliza un deepfake de un gerente para emitir órdenes falsas a personal de seguridad y solicitar acceso a zonas restringidas, logrando que el guardia valide la identidad visual sin detectar el fraude.

Sabotaje OT: Implica el ingreso físico a la planta, colocación de USB o hardware malicioso, modificación de parámetros de control industrial, lo que ocasiona fallas, paros o accidentes.

Ataques coordinados: Se genera una distracción física (incendio, fuga, manifestación falsa) que facilita la extracción de datos, desactivación de cámaras, penetración de redes internas y manipulación de sensores IoT.

Soluciones avanzadas

SIEM unificado físico-digital: Un sistema que correlaciona accesos físicos, registros de CCTV, logs IT, eventos OT y alertas de intrusión, permitiendo detectar patrones imposibles de identificar en sistemas aislados.

Autenticación multifactor física: Incorporación de biométricos, PIN dinámicos, tokens y verificación de comportamiento.

Capacitación en ingeniería social avanzada: Preparación para enfrentar amenazas como deepfakes, voces clonadas, correos personalizados y ataques de coerción y manipulación emocional.

Alcance

Este modelo resulta aplicable a centros de distribución, plantas industriales, instalaciones con integración OT/IT, infraestructura crítica, aeropuertos y puertos.

Conclusión

Los ataques híbridos se han convertido en la norma. La seguridad moderna debe ser convergente, integrando lo físico, lo digital y lo humano en un único ecosistema defensivo.

Simulacros Psicológicos: Más Allá del Procedimiento

Introducción

Los simulacros tradicionales suelen enfocarse en cumplir normativas, sin evaluar la reacción real del personal ante situaciones de estrés. Las personas se comportan de manera diferente bajo presión, y la única forma de medir esa respuesta genuina es a través de escenarios inmersivos.

Objetivo

El objetivo es crear simulacros que reproduzcan condiciones cognitivas y emocionales similares a una emergencia real, posibilitando la evaluación de liderazgo, toma de decisiones, reacción ante el pánico, coordinación y resiliencia de los equipos.

Desarrollo

Limitaciones de los simulacros tradicionales

Los simulacros convencionales presentan varias carencias: son anunciados con antelación, carecen de presión real, no incorporan elementos de caos o ambigüedad, no miden la respuesta emocional, no identifican líderes naturales ni detectan fallas humanas auténticas.

Modelo de simulación inmersiva

Elementos sorpresa: Se incluyen alarmas inesperadas, participación de actores externos, herramientas sensoriales como humo frío y ruido, desorientación moderada y fallas simuladas de sistemas.

Estímulos sensoriales: Estos aumentan el realismo y activan respuestas autónomas, facilitando la medición de pánico, reacción inmediata y comunicación bajo estrés.

Monitoreo conductual: Empleo de cámaras de estudio, mapas de calor de movimiento, cronometraje de decisiones y análisis de voz bajo condiciones de estrés.

Caso práctico

Tras la realización de tres simulacros inmersivos, se observó una reducción del tiempo de evacuación en un 42%, identificación de líderes emergentes, optimización de rutas de salida y mejora en la coordinación entre distintas áreas.

Alcance

Este enfoque es adecuado para edificios corporativos, centros comerciales, plantas industriales, centros educativos y hospitales.

Conclusión

El comportamiento humano es el factor más crítico en una crisis. Los simulacros psicológicos permiten medir lo que realmente importa: la respuesta humana auténtica ante situaciones de emergencia.

Riesgo Reputacional: Cuando el Daño No es Físico, pero es Real

Introducción

En el contexto actual de la era digital, los incidentes de seguridad han dejado de limitarse únicamente a los activos físicos o digitales. Ahora, el impacto se extiende a la percepción pública de la marca y afecta directamente la confianza de clientes, inversionistas y autoridades. Un video viral, una gestión comunicacional deficiente o el silencio prolongado posterior a un incidente pueden resultar más perjudiciales que el propio evento. Por ello, la gestión del riesgo reputacional se posiciona como un pilar esencial en la seguridad corporativa moderna.

Objetivo

El propósito central es desarrollar un modelo de gestión reputacional que permita anticiparse, monitorear, contener y recuperar la imagen institucional ante incidentes vinculados a la seguridad física o digital.

- La reputación como activo de alto valor
- La reputación empresarial es un activo intangible que genera impactos tangibles en múltiples áreas:
- Ventas
- Relaciones comerciales
- Valor de marca
- Negociaciones con aseguradoras
- Regulaciones y auditorías
- Credibilidad ante stakeholders

La rapidez con la que puede deteriorarse la reputación en un entorno hiperconectado convierte a este activo en un elemento crítico que puede verse afectado en cuestión de minutos.

Mapa de Riesgos Reputacionales

La clasificación de los incidentes según el impacto mediático potencial es fundamental. Entre los escenarios contemplados se incluyen:

- Agresiones o robos dentro de instalaciones
- Filtraciones de video donde el personal de seguridad actúa de manera inapropiada
- Fallas en controles de acceso
- Casos de discriminación, reales o percibidos
- Violaciones de datos de clientes
- Crisis con proveedores o personal externo

Para cada uno de estos escenarios se cuenta con un protocolo comunicacional previamente diseñado, lo que permite responder de manera rápida y efectiva.

Monitoreo en tiempo real

El uso de herramientas de escucha social apoyadas por inteligencia artificial es clave para:

- Detectar publicaciones virales
- Identificar hashtags emergentes
- Medir el nivel de indignación pública
- Clasificar el sentimiento (positivo, neutro, negativo)
- Generar alertas automáticas para el gabinete de crisis

Este monitoreo en tiempo real permite actuar de forma proactiva y minimizar el daño reputacional.

Protocolos de comunicación rápida

- Los protocolos de comunicación ante crisis reputacional contemplan:
- Emisión de mensajes iniciales en un máximo de 30 minutos
- Designación de un vocero único y capacitado
- Manejo de una narrativa transparente (qué ocurrió, qué se está haciendo, qué se garantiza)
- Evitar la especulación
- Coordinación en la publicación de información en redes internas y externas

Simulacros de crisis reputacional

La realización de simulacros incluye diversos escenarios como filtros falsos en redes sociales, videos alterados, entrevistas espontáneas, llamadas de medios y presión tanto interna como externa. Estos ejercicios permiten evaluar la madurez y preparación del equipo directivo frente a una crisis real.

Caso real

En un caso específico, una empresa enfrentó la difusión de un video que mostraba una supuesta agresión por parte de un guardia de seguridad. Gracias al monitoreo en tiempo real y la aplicación del protocolo reactivo, se logró emitir un comunicado verificado en 55 minutos, liberar evidencia completa, confirmar la manipulación del video y controlar la narrativa en menos de dos horas.

Alcance

El modelo de gestión reputacional es aplicable a empresas con atención al público, retail, transporte, seguridad privada y corporativos de todo tipo de industrias.

Conclusión

La protección de la reputación institucional depende de la velocidad de reacción, la transparencia y la preparación. Aquellas organizaciones que no gestionan el riesgo reputacional quedan expuestas a daños que pueden perdurar por años.

Seguridad Inclusiva: Sin Sesgos, Sin Discriminación

Introducción

La seguridad moderna, además de ser eficiente, debe ser ética. Un sistema que discrimina o perfila injustamente no solo pierde eficiencia, sino que expone a la organización a riesgos legales, reputacionales y operativos. La seguridad inclusiva es una tendencia global que promueve controles basados en el riesgo real y no en prejuicios.

Objetivo

Garantizar que los controles de seguridad sean equitativos, éticos y libres de sesgos, con el fin de mejorar la experiencia de los usuarios, fortalecer la cultura organizacional y reducir riesgos legales.

Identificación de sesgos en seguridad

Los sesgos pueden manifestarse en diferentes etapas del proceso de seguridad, incluyendo:

- Revisión de personas por “apariencia”

- Selección de candidatos
- Evaluación de proveedores
- Interpretación de comportamientos
- Algoritmos de reconocimiento facial o scoring
- Estos sesgos distorsionan la percepción y gestión del riesgo.

Auditoría de sesgos en algoritmos

La auditoría se aplica a sistemas como reconocimiento facial, modelos de scoring de visitantes y sistemas de detección de anomalías. Se evalúan aspectos como:

- Datos de entrenamiento
- Diversidad de la base
- Tasa de falsos positivos por grupo demográfico
- Nivel de equidad estadística
- Capacitación en inclusión
- El personal de seguridad recibe formación para:
- Identificar sesgos inconscientes
- Tratar a todas las personas con dignidad
- Aplicar controles con lenguaje neutral
- Manejar situaciones sensibles

Revisión aleatoria consciente

Las revisiones se basan en criterios objetivos, como el nivel de riesgo de la operación, políticas internas y flujo de visitantes, evitando criterios basados en apariencia, origen o clase social.

Encuestas de percepción

Las encuestas permiten identificar sensaciones de trato inequitativo, falta de claridad en los controles y posibles fricciones entre visitantes o empleados.

Indicador de equidad

Se realiza una comparación entre el número de revisiones aplicadas y los indicios reales de incidentes, con el objetivo de evitar revisiones injustificadas.

Alcance

El enfoque de seguridad inclusiva es aplicable en corporativos, retail, industria, escuelas, hospitales y empresas de seguridad privada.

Conclusión

La seguridad justa es sinónimo de seguridad efectiva. La inclusión no disminuye la protección, sino que la mejora al eliminar decisiones erróneas basadas en prejuicios.

Security by Design: Construir Seguro desde el Plano

Introducción

Incorporar la seguridad desde la fase arquitectónica no solo reduce costos, sino que evita la necesidad de rediseños posteriores. El enfoque Security by Design integra controles estructurales, tecnológicos y operativos desde el inicio del proyecto.

Objetivo

El objetivo es asegurar que las construcciones, remodelaciones y expansiones incluyan medidas de seguridad desde el diseño, optimizando recursos y minimizando riesgos.

Evaluación geoespacial

La evaluación geoespacial contempla:

- Análisis delictivo del área
- Rutas seguras de acceso
- Iluminación pública
- Riesgos naturales
- Flujos vehiculares y peatonales

Zonificación por nivel de riesgo

La zonificación divide las áreas en:

- Zonas públicas
- Semi públicas
- Controladas
- Críticas
- Ultra restringidas
- Con ello se define el flujo humano ideal para cada zona.

Elementos pasivos

- Los elementos pasivos incluyen:
- Muros antiblast

- Control natural de accesos
- Vegetación como barrera anti-intrusión
- Ventanas reforzadas
- Barreras vehiculares integradas estéticamente

Simulaciones 3D

Las simulaciones permiten visualizar rutas de evacuación, probar flujos en caso de incendio o desastre, identificar cuellos de botella y validar accesos de emergencia.

Caso práctico

La implementación de Security by Design permitió a una empresa integrar vigilancia natural, reducir puntos ciegos, mejorar la accesibilidad y disminuir los costos de seguridad en un 40%.

Alcance

Este enfoque es aplicable en parques industriales, corporativos, centros comerciales, hospitales, escuelas e infraestructura crítica.

Conclusión

Diseñar con seguridad desde la etapa inicial maximiza la eficiencia, reduce gastos y contribuye a crear instalaciones más resilientes.

Red Team Interno: Atacar para Defender

Introducción

Los ataques simulados son herramientas clave para evaluar la efectividad real de los controles de seguridad. Un Red Team interno replica las estrategias de atacantes reales para detectar vulnerabilidades.

Objetivo

Medir la capacidad de detección, reacción y resiliencia de los sistemas de seguridad mediante ataques controlados y recurrentes.

Selección de talento

- Un equipo de Red Team eficaz requiere:
- Pensamiento creativo
- Perfil analítico
- Capacidad de improvisación
- Conocimiento técnico físico y digital

Técnicas de ataque

Las técnicas incluyen:

- Ingeniería social
- Ingreso físico
- Manipulación de sistemas OT
- Suplantación de identidades
- Colocación de dispositivos

Campañas sorpresivas

De forma mensual se ejecutan ataques simulados, tales como:

- Intento de acceso con credenciales falsas
- Pruebas de tailgating
- Penetración mediante errores humanos
- Extracción simulada de datos
- Plantación de dispositivos USB

Rotación con equipos externos

La rotación con equipos externos evita la familiaridad y ayuda a detectar nuevas vulnerabilidades.

Caso práctico

En un ejercicio, el Red Team detectó que los guardias aprobaban accesos visuales sin validar credenciales, el sistema permitía la duplicación de llaves y la capacitación era insuficiente. Tras aplicar correcciones, se cerró la brecha crítica.

Alcance

La estrategia es aplicable en logística, industria, retail e infraestructura crítica.

Conclusión

Atacar para defender es una estrategia moderna que permite descubrir brechas antes de que lo haga un actor malicioso.

KPIs Predictivos: Del “Qué Pasó” al “Qué Pasará”

Introducción

Si bien la seguridad tradicional se basa en indicadores históricos, la seguridad moderna demanda anticipación. Los KPIs predictivos permiten actuar antes de que ocurra un incidente.

Objetivo

Desarrollar indicadores capaces de anticipar incidentes utilizando analítica avanzada, detección de anomalías y modelos de riesgo en tiempo real.

Limitaciones de indicadores tradicionales

Los indicadores tradicionales únicamente miden:

- Eventos pasados
- Tiempos de respuesta
- Incidentes ya consumados
- No contribuyen a la prevención.

Modelo predictivo

El modelo predictivo integra:

- Machine learning
- Tendencias delictivas externas
- Comportamiento anómalo interno
- Sensores IoT
- Patrones geográficos

Puntuación dinámica de riesgo

La puntuación de riesgo se actualiza cada 24 horas considerando:

- Eventos del día anterior
- Cambios en personal, rutas o proveedores
- Noticias locales
- Reportes operativos

Alertas preventivas

El sistema genera alertas en los siguientes casos:

- Comportamientos fuera del estándar
- Desviaciones en accesos
- Riesgo creciente en una zona

Caso práctico

Al implementar KPIs predictivos, los robos internos se redujeron un 35%, se detectaron anomalías con días de anticipación y se priorizaron áreas críticas con mayor precisión.

Alcance

La aplicación de KPIs predictivos es relevante en logística, manufactura, retail, salud y servicios.

Conclusión

Estos indicadores convierten la seguridad en un proceso proactivo, logrando reducir incidentes antes de que sucedan.

Personal Invisible: El Riesgo que No Ves

Introducción

Los servicios de limpieza, mantenimiento, jardinería y personal temporal suelen operar con mayor libertad y menor supervisión, lo que los convierte en un "personal invisible" y en uno de los riesgos más ignorados y críticos.

Objetivo

Establecer controles que aseguren visibilidad, trazabilidad y control sobre las actividades del personal externo de soporte.

Riesgos asociados

Los riesgos incluyen:

- Acceso a áreas sensibles
- Manejo de herramientas
- Movilidad sin supervisión
- Posesión de información operativa
- Colocación de dispositivos maliciosos

Registro detallado por tarea

Cada actividad debe contemplar:

- Responsable
- Hora de inicio y fin
- Área específica
- Materiales usados
- Validación del supervisor

Credenciales temporales con QR dinámico

Este sistema permite:

- Revocar acceso en tiempo real
- Monitorear ubicación por zonas
- Visualizar historial de movimientos
- Registrar accesos con precisión

Zonas restringidas

El acceso a zonas restringidas debe estar bajo acompañamiento, supervisión directa y permisos temporales.

Revisión de herramientas

La revisión de herramientas tiene como objetivo evitar el ocultamiento de dispositivos, la plantación de hardware y el robo de equipo crítico.

Alcance

Este modelo es aplicable en cualquier instalación con presencia continua de personal externo.

Conclusión

Controlar al “personal invisible” ayuda a disminuir ataques internos y la fuga de información sin generar fricción operativa significativa.

Seguridad en la Era de la Inteligencia Artificial: Cuando el Ataque También Piensa

Introducción

La inteligencia artificial (IA) ha modificado radicalmente tanto los mecanismos de defensa como las estrategias de ataque en el entorno de la seguridad. Actualmente, los delincuentes emplean IA para realizar acciones como la clonación de voces, la falsificación de identidades, la automatización de intrusiones y la manipulación de sistemas biométricos. Ante este panorama, resulta indispensable que las organizaciones se preparen para enfrentar amenazas inteligentes capaces de superar los controles tradicionales.

Objetivo

El objetivo principal es implementar mecanismos sólidos que protejan a la organización frente a amenazas potenciadas por el uso malicioso de inteligencia

artificial. Solo así se podrá mantener la integridad, confidencialidad y disponibilidad de los activos organizacionales.

Tipos de ataques impulsados por IA

Los ataques basados en IA se presentan en diversas formas sofisticadas:

Deepfakes: Generación de imágenes y videos falsos altamente realistas para engañar a personas y sistemas.

Clonación de voz: Imitación de voces legítimas para obtener acceso no autorizado o manipular procesos críticos.

Suplantación biométrica: Manipulación de datos biométricos para burlar controles de acceso.

Optimización de ataques cibernéticos: Automatización y mejora continua de técnicas de intrusión mediante IA.

Ingeniería social automatizada: Uso de IA para personalizar ataques y aumentar su efectividad.

Creación de identidades sintéticas: Fabricación de perfiles falsos complejos para infiltrarse en sistemas y redes.

Actualización continua de algoritmos defensivos

La defensa ante amenazas impulsadas por IA requiere mantener los algoritmos en constante evolución. Es fundamental reentrenar modelos de detección, incorporar nuevas muestras de ataques, verificar la precisión de los sistemas y eliminar sesgos que puedan ser explotados por actores maliciosos.

Validación multimodal

Para reforzar la autenticación, es necesario combinar diferentes factores de verificación de manera simultánea. Esto incluye la evaluación de rostro, voz, comportamiento del usuario, credenciales físicas y factores contextuales como ubicación y horario. La validación multimodal dificulta la suplantación, ya que exige superar múltiples barreras de seguridad a la vez.

Anti-spoofing

Los sistemas anti-spoofing deben ser capaces de detectar si se trata de piel real, identificar latidos faciales, encontrar inconsistencias en sombras y evaluar patrones de microexpresiones. Estas capacidades permiten diferenciar entre una persona legítima y un intento de engaño elaborado con IA.

Simulacros de ataque con IA

La realización de simulacros de ataque que emplean IA es esencial para evaluar la preparación de la organización. Estos ejercicios pueden incluir llamadas falsas de ejecutivos, videos manipulados, órdenes apócrifas o la suplantación de identidad en videoconferencias, lo que ayuda a identificar vulnerabilidades y fortalecer los protocolos de respuesta.

Alcance

La implementación de estas medidas es indispensable en sectores como corporativos, bancos, retail, gobierno e infraestructura crítica, donde la exposición al riesgo es mayor y las consecuencias de un ataque exitoso pueden ser graves.

Conclusión

La inteligencia artificial no solo protege, también representa una herramienta poderosa para los atacantes. Prepararse para enfrentar estas nuevas amenazas es clave para definir la resiliencia futura de las organizaciones.

Referencias:

ASIS / Seguridad Física

ASIS International. (s.f.). *Physical Asset Protection (PAP).* ASIS International.
ASIS International. (s.f.). *Physical Security Professional (PSP) Reference Material.* ASIS International.
ASIS International. (s.f.). *Protection of Assets Manual (POA).* ASIS International.

NFPA

National Fire Protection Association. (s.f.). *NFPA 730: Guide for Premises Security.* NFPA.
National Fire Protection Association. (s.f.). *NFPA 731: Standard for the Installation of Electronic Premises Security Systems.* NFPA.
National Fire Protection Association. (s.f.). *NFPA 72: National Fire Alarm and Signaling Code.* NFPA.
National Fire Protection Association. (s.f.). *NFPA 1: Fire Code.* NFPA.
National Fire Protection Association. (s.f.). *NFPA 101: Life Safety Code.* NFPA.
National Fire Protection Association. (s.f.). *NFPA 10: Portable Fire Extinguishers.* NFPA.
National Fire Protection Association. (s.f.). *NFPA 25: Inspection, Testing & Maintenance of Water-Based Systems.* NFPA.
National Fire Protection Association. (s.f.). *NFPA 1600: Continuity, Emergency & Crisis Management.* NFPA.

UL

Underwriters Laboratories. (s.f.). *UL 294: Standard for Access Control System Units.* UL Standards.
Underwriters Laboratories. (s.f.). *UL 2050: National Industrial Security Systems (NISPOM).* UL Standards.

ISO

International Organization for Standardization. (2021). *ISO 22341: Guidelines for crime prevention through environmental design (CPTED).* ISO.
International Organization for Standardization. (2018). *ISO 31000: Risk Management – Guidelines.* ISO.
International Organization for Standardization. (2007). *ISO 28000: Specification for security management systems for the supply chain.* ISO.
International Organization for Standardization. (2007). *ISO 28001: Best practices for implementing supply chain security.* ISO.
International Organization for Standardization. (2018). *ISO 31010: Risk Assessment Techniques.* ISO.
International Organization for Standardization. (2018). *ISO 22320: Emergency Management – Guidelines.* ISO.
International Organization for Standardization. (2018). *ISO 22324: Emergency Colour Coding for Alerts.* ISO.
International Organization for Standardization. (2015). *ISO 22315: Guidelines for mass evacuation.* ISO.
International Organization for Standardization. (2019). *ISO 22301: Security and resilience – Business continuity management systems.* ISO.
International Organization for Standardization. (2020). *ISO 22313: Guidance for business continuity management systems.* ISO.
International Organization for Standardization. (2015). *ISO 18788: Management System for Private Security Operations.* ISO.

ANSI / UNE / FM / OSHA

American National Standards Institute. (s.f.). *Facility Safety Design Guidelines.* ANSI.
Asociación Española de Normalización. (s.f.). *UNE 192005: Seguridad en las organizaciones.* UNE.
FM Global. (s.f.). *Property Loss Prevention Data Sheets.* FM Global.
Occupational Safety and Health Administration. (s.f.). *29 CFR 1910: General Industry Standards.* U.S. Department of Labor.

Cadena de Suministro: BASC, OEA, CTPAT

World BASC Organization. (2022). *Norma y Estándares Internacionales BASC Versión 6-2022.* BASC.
World Customs Organization. (s.f.). *SAFE Framework of Standards: Authorized Economic Operator (AEO/OEA).* WCO.
U.S. Customs and Border Protection. (s.f.). *C-TPAT Minimum Security Criteria.* CBP.

OEA & C-TPAT. (s.f.). *Requisitos de subcontratación segura.* WCO & CBP.

CCTV y Sistemas Electrónicos

International Electrotechnical Commission. (s.f.). *IEC 62676: Video Surveillance Systems Standards.* IEC.
ONVIF. (s.f.). *ONVIF Profiles S, G & T – Interoperability Standards.* ONVIF.
European Committee for Standardization. (s.f.). *EN 50132: CCTV in security applications.* CEN.

Modelos de Riesgos y Metodologías

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise Risk Management Framework (COSO ERM).* COSO.
Sandia National Laboratories. (s.f.). *RAM-W, RAM-CF & RAM-KS Methodologies.* Sandia Labs.
U.S. Department of Homeland Security. (s.f.). *Security Vulnerability Assessment (SVA) Guidelines.* DHS.
National Institute of Standards and Technology. (2012). *NIST SP 800-30: Guide for Conducting Risk Assessments.* NIST.

Riesgos Naturales

Federal Emergency Management Agency. (s.f.). *Hazard Mitigation Planning Guides.* FEMA.
United States Geological Survey. (s.f.). *Earthquake and Natural Hazard Models.* USGS.
National Oceanic and Atmospheric Administration. (s.f.). *Severe Weather Preparedness Guidelines.* NOAA.
United Nations Office for Disaster Risk Reduction. (2015). *Sendai Framework for Disaster Risk Reduction 2015–2030.* UNDRR.
Centro Nacional de Prevención de Desastres. (s.f.). *Guías de Gestión de Riesgos Naturales.* CENAPRED.

Inteligencia de Amenazas y Riesgo Social

Overseas Security Advisory Council. (s.f.). *Security and Crime Reports.* U.S. Department of State.

United Nations Office on Drugs and Crime. (s.f.). *Crime and Safety Reports.* UNODC.
Instituto Nacional de Estadística y Geografía. (s.f.). *Encuesta Nacional de Seguridad Urbana.* INEGI.
Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (s.f.). *Reportes de incidencia delictiva.* SESNSP.
CompStat. (s.f.). *Hotspot Crime Analysis Models.* NYPD.

Proveedores de Seguridad / KPI

ASIS International. (s.f.). *Private Security Officer Selection and Training Guideline.* ASIS.
ASIS International. (s.f.). *Security Officer Metrics & KPIs Manual.* ASIS.
American National Standards Institute & ASIS International. (2012). *ANSI/ASIS PSC.1: Operational Guidelines for Private Security Providers.* ANSI/ASIS.